

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-146761
 (43)Date of publication of application : 06.06.1997

(51)Int.CI. G06F 7/58

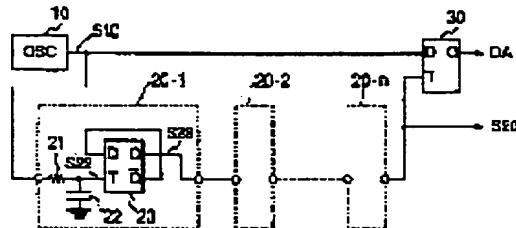
(21)Application number : 07-308594 (71)Applicant : OKI ELECTRIC IND CO LTD
 KOKUSAI GIJUTSU KAIHATSU KK
 (22)Date of filing : 28.11.1995 (72)Inventor : TAKEMOTO MITSUO

(54) RANDOM NUMBER GENERATION CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To attain low power consumption and to obtain highly reliable random number data by supplying power only at the time of using the random number generation circuit.

SOLUTION: When a power supply is turned on, an oscillation output signal S10 is outputted from an oscillation circuit(OSC) 10. The output signal S10 is integrated to a triangular wave shape by a CR integration circuit consisting of a resistor 21 and a capacitor 22 in an initial two-frequency dividing circuit 20-1, the integration signal S22 is divided into two frequency components by a D-FF 23, output data S23 are outputted from the D-FF 23 and successively sent to succeeding two-frequency division circuits 20-2 to 20-n. Thereby jitter due to ambient noise is successively amplified an a clock signal S20 having jitter width larger than the half period of the output signal S10 is outputted from the final two-frequency division circuit 20-n. A D-FF 30 samples the output signal S10 based upon the clock signal S20 and outputs random number data DA consisting of '0' and '1'.



LEGAL STATUS

[Date of request for examination] 30.03.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3294489

[Date of registration] 05.04.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-146761

(43) 公開日 平成9年(1997)6月6日

(51) Int.Cl.⁶

G 0 6 F 7/58

識別記号

庁内整理番号

F I

C 0 6 F 7/58

技術表示箇所

△

審査請求 未請求 請求項の数 5 O L (全 7 頁)

(21) 出願番号

特願平7-308594

(22) 出願日

平成7年(1995)11月28日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(71) 出願人 000170554

国際技術開発株式会社

東京都杉並区天沼2丁目3番9号

(72) 発明者 竹本 光雄

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

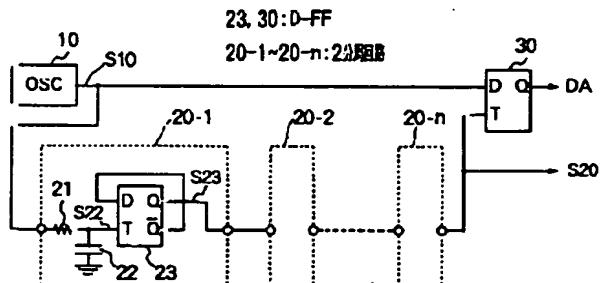
(74) 代理人 弁理士 柿本 恭成

(54) 【発明の名称】 亂数発生回路

(57) 【要約】

【課題】 使用時のみ電源を投入して低消費電力化を図り、信頼性の高い乱数データを得る。

【解決手段】 電源投入によって発振回路(ОСC)10から発振出力信号S10が出力される。初段の2分周回路20-1内の抵抗21及びコンデンサ22からなるC-R積分回路により、出力信号S10が三角波状に積分され、この積分信号S22がD-FF23で2分周され、該D-FF23から出力データS23が出力され、次段の2分周回路20-2～20-nへ順次送られていく。これにより、周囲雑音によるジッタが順次増幅され、出力信号S10の半周期よりも大きなジッタ幅を有するクロック信号S20が、最終段の2分周回路20-nから出力される。D-FF30では、クロック信号S20によって出力信号S10をサンプリングし、“0”、“1”の乱数データDAを出力する。



本発明の第1の実施形態の乱数発生回路

【特許請求の範囲】

【請求項1】 電源の投入によって一定の周波数で発振する発振手段と、

前記発振手段の出力信号に基づき、該出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成して出力するクロック生成手段と、前記クロック生成手段の出力信号中のジッタによって前記発振手段の出力信号をサンプリングし、論理信号からなる乱数データを出力するサンプリング手段とを、備えたことを特徴とする乱数発生回路。

【請求項2】 電源の投入によって一定の周波数で発振する第1の発振手段と、

前記電源の投入により、前記第1の発振手段に対して非整数倍の周波数で発振する第2の発振手段と、

前記第2の発振手段の出力信号に基づき、前記第1の発振手段の出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成して出力するクロック生成手段と、

前記クロック生成手段の出力信号中のジッタによって前記第1の発振手段の出力信号をサンプリングし、論理信号からなる乱数データを出力するサンプリング手段とを、

備えたことを特徴とする乱数発生回路。

【請求項3】 請求項1又は2記載の乱数発生回路と、前記サンプリング手段の出力データをスクランブルして該スクランブルされた乱数データを出力するスクランブル回路とを、

備えたことを特徴とする乱数発生回路。

【請求項4】 請求項1、2又は3記載の乱数発生回路において、

前記クロック生成手段は、複数段の分周回路で構成し、前記各段の分周回路は、請求項1の発振手段の出力信号又は請求項2の第2の発振手段の出力信号を積分する抵抗及びコンデンサからなる積分回路と、前記積分回路の出力信号をクロック入力として該出力信号を分周する分周カウンタとで、構成したことを特徴とする乱数発生回路。

【請求項5】 請求項1、2又は3記載の乱数発生回路において、

前記サンプリング手段は、前記クロック生成手段の出力信号をクロック入力として、請求項1の発振手段の出力信号又は請求項2の第1の発振手段の出力信号を取込んで前記乱数データを出力するフリップフロップ回路で構成したことを特徴とする乱数発生回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、マイクロコンピュータを搭載した電池駆動の携帯用電子機器と、マイクロコンピュータを搭載した装置との間で、データ伝送を行う場合、これらの携帯用電子機器及び装置にそ

れぞれ設けられ、秘密保持の見地から伝送すべきデータを暗号化するため等に用いられる乱数発生回路に関するものである。

【0002】

【従来の技術】図2は従来の乱数発生回路の概略の構成図、及び図3はその図2の暗号化処理を示す図である。図2の乱数発生回路は、一定の周波数で発振する発振回路（以下、「OSC」という）1と、該OSC1の出力信号を分周して出力データ（即ち、乱数データ）DAを出力する時計等の自走カウンタ2とで、構成されている。自走カウンタ2の出力データDAは、図示しない中央処理装置（以下、「CPU」という）で読み取られ、該CPUで演算処理が行われて送信すべきデータが暗号化され、外部へ送信されるようになっている。図3では、自走カウンタ2の出力データDAをCPUが任意の時点で読み込むことが示されている。図2の乱数発生回路を搭載した装置に電源が供給されると、該電源が供給された任意の時点から自走カウンタ2がカウント動作を開始し、さらに、この装置が使用される任意の時点から、CPUによる一定のプログラム処理後に、該CPUが自走カウンタ2の出力データDA（例えば、D_{n+1}）を読み込むことで乱数データを得ている。CPUは、読み込んだ乱数データに演算処理を施して送信すべきデータを暗号化し、図示しない送信部から外部へ送出させる。

【0003】

【発明が解決しようとする課題】しかしながら、従来の乱数発生回路では、次のような問題があり、これを解決することが困難であった。

(a) 図2の乱数発生回路では、ランダムな出力データDA、即ち乱数データを得るために、OSC1及び自走カウンタ2に対して常時電源電力を供給して動作させておかなければならない。そのため、図2の乱数発生回路を搭載した装置が例えば電池駆動の場合、この電池の寿命が短くなる、つまり消費電力が大きいという問題がある。

(b) 前記(a)の消費電力を小さくするために、例えば、装置の使用時のみ電源電力を供給するという方法も考えられる。この方法の場合、CPUが出力データDAを読み込むタイミングが、電源を投入したときから該CPUが読み込みの準備のために一定のプログラム処理をするので、ある規則性がある。また、自走カウンタ2の出力データDAの値も、電源の投入から一定時間後はある規則性を持つ。そのため、CPUが読み込む出力データDAの値は、一定の規則性を持ってしまい、充分な乱数にならなくなってしまう。

本発明は、前記従来技術が持っていた課題を解決し、例えば、使用時のみ電源を投入して低消費電力化を図ると共に、信頼性の高い乱数データを得ることができる乱数発生回路を提供するものである。

【0004】

【課題を解決するための手段】前記課題を解決するためには、第1の発明は、データ伝送装置等の種々の装置に設けられる乱数発生回路において、電源の投入によって一定の周波数で発振する発振手段（例えば、発振回路）と、前記発振手段の出力信号に基づき、該出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成して出力するクロック生成手段（例えば、複数段の分周回路等で構成）と、前記クロック生成手段の出力信号中のジッタによって前記発振手段の出力信号をサンプリングし、論理信号（例えば、“1”、“0”）からなる乱数データを出力するサンプリング手段（例えば、フリップフロップ回路等）とを、備えている。第2の発明は、乱数発生回路において、電源の投入によって一定の周波数で発振する第1の発振手段と、前記電源の投入により、前記第1の発振手段に対して非整数倍の周波数で発振する第2の発振手段と、前記第2の発振手段の出力信号に基づき、前記第1の発振手段の出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成して出力するクロック生成手段と、前記クロック生成手段の出力信号中のジッタによって前記第1の発振手段の出力信号をサンプリングし、論理信号からなる乱数データを出力するサンプリング手段とを、備えている。第3の発明は、第1又は第2の発明の乱数発生回路と、前記サンプリング手段の出力データをスクランブルして該スクランブルされた乱数データを出力するスクランブル回路とを、備えている。

【0005】第1の発明によれば、以上のように乱数発生回路を構成したので、電源を投入すると、発振手段が一定の周波数で発振して該発振出力信号がクロック生成手段及びサンプリング手段へ送られる。クロック生成手段では、発振手段の出力信号を入力し、例えば、ジッタを含んだクロック信号を生成し、このジッタを増幅して該出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成し、サンプリング手段へ送る。サンプリング手段では、クロック生成手段の出力信号中のジッタによって発振手段の出力信号をサンプリングし、乱数データを出力する。第2の発明によれば、電源を投入すると、第1の発振手段と第2の発振手段とがそれぞれ非同期に発振し、この第1の発振手段の出力信号がサンプリング手段へ送られ、第2の発振手段の出力信号がクロック生成手段へ送られる。クロック生成手段では、第2の発振手段の出力信号を入力し、第1の発振手段の出力信号の半周期よりも大きなジッタ幅を有するクロック信号を生成し、サンプリング手段へ送る。サンプリング手段では、クロック生成手段の出力信号中のジッタによって第1の発振手段の出力信号をサンプリングし、乱数データを出力する。第3の発明によれば、電源の投入によって第1又は第2の発明のサンプリング手段から出力された出力データが、スクランブル回路へ送られ、該スクランブル回路によって該出力データがスクランブルされ、

乱数データが出力される。

【0006】

【発明の実施の形態】

第1の実施形態

図1は、本発明の第1の実施形態を示す乱数発生回路の構成図である。この乱数発生回路は、発振手段（例えば、OSC10）と、該OSC10の出力側に接続されたクロック生成手段（例えば、複数（n）段の2分周回路）20-1～20-nと、該OSC10及び最終段の2分周回路20-nの出力側に接続されたサンプリング手段（例えば、D型フリップフロップ回路、以下これを「D-F F」という）30とで、構成されている。OSC10は、電源の投入によって一定の周波数で発振して出力信号S10を出力する回路であり、水晶発振回路等で構成されている。クロック生成手段を構成するn段の2分周回路20-1～20-nは、出力信号S10を入力し、該出力信号S10の半周期よりも大きなジッタ幅を有するクロック信号S20を生成してD-F F30へ与える回路であり、これら各段の2分周回路20-1～20-nが同一回路で構成されている。

【0007】例えば、初段の2分周回路20-1は、出力信号S10を三角波状に積分する抵抗21及びコンデンサ22からなるCR積分回路と、該CR積分回路から出力される積分信号S22を波形整形のために2分周する2分周カウンタ（例えば、D-F F）23とで、構成されている。D-F F23は、データ入力端子D、クロック入力端子T、出力信号S23を出力するデータ出力端子Q、及び反転データ出力端子Q/を有し、該クロック入力端子Tが抵抗21及びコンデンサ22の接続点に接続され、該データ入力端子Dが反転データ出力端子Q/に接続されている。D-F F23のデータ出力端子Qは、次段の2分周回路20-2内の抵抗に接続されている。同様に、他の2分周回路20-3～20-nが継続接続され、この最終段の2分周回路20-n内のD-F Fのデータ出力端子がD-F F30に接続されている。D-F F30は、データ入力端子D、クロック入力端子T、及びデータ出力端子Qを有し、該データ入力端子DがOSC10の出力側に接続され、該クロック入力端子Tが最終段の2分周回路20-n内のD-F Fのデータ出力端子に接続され、データ出力端子Qから“1”、“0”的出力データ（即ち、乱数データ）DAを出力する回路である。

【0008】図4及び図5は、図1に示す乱数発生回路の動作波形図であり、これらの図を参照しつつ、図1の乱数発生回路の動作を説明する。電源を投入すると、OSC10が発振動作を開始し、このOSC10から一定の周波数の出力信号S10が出力され、D-F F30及び初段の2分周回路20-1へ送られる。初段の2分周回路20-1では、入力された出力信号S10が、抵抗21及びコンデンサ22からなるCR積分回路によって

三角波状に積分され、該C R 積分回路から積分信号S 2 2が outputされる。C R 積分回路は、抵抗2 1の抵抗値を大きくすると共にコンデンサ2 2の容量値を小さくすれば、インピーダンスが大きくなつて周囲雑音を拾いやすくなる。そのため、出力信号S 1 0を、抵抗2 1及びコンデンサ2 2で積分して三角波状の積分信号S 2 2にすることにより、D - F F 2 3のクロック入力端子Tから見て、変換点に周囲雑音によるジッタを含んだ信号となる。D - F F 2 3は、ジッタを含んだ積分信号S 2 2を、波形整形のために2分周する。この結果、D - F F 2 3のデータ出力端子Qから出力される出力信号S 2 3も、ジッタを含んだ信号となる。この出力信号S 2 3は、次段の2分周回路2 0 - 2へ送られ、初段の2分周回路2 0 - 1と同様にしてジッタがさらに増大されて出力され、次段の2分周回路2 0 - 3へ送られる。このようにして、ジッタが増幅され、最終段の2分周回路2 0 - nから、出力信号S 1 0の半周期よりジッタ幅が大きいクロック信号S 2 0が outputされ、D - F F 3 0のクロック入力端子Tへ送られる。

【0009】D - F F 3 0では、クロック信号S 1 0のジッタにより、OSC 1 0の出力信号S 1 0をサンプリングする。即ち、図5に示すクロック信号S 2 0の立上がり箇所のジッタの、いずれかの立上がりにより、出力信号S 1 0がサンプリングされ、D - F F 3 0のデータ出力端子Qから、出力データDAが outputされる。この出力データDAでは、例えば、クロック信号S 2 0中のジッタのいずれかの立上がりに対応して、データD₁とD₂の境界が決定されるため、該出力データDAが乱数データとなる。即ち、D - F F 3 0のデータ入力端子Dに入力される出力信号S 1 0の“1”と“0”的区間をまたがって、入力されるクロック信号S 2 0のジッタがあるため、該D - F F 3 0のデータ出力端子Qから出力される出力データDAが、乱数データとなる。D - F F 3 0から出力された乱数データは、図示しないCPU等で読み込まれ、該CPU等の演算処理によって伝送すべきデータが暗号化され、この暗号化されたデータが、図示しない送信部から外部へ出力される。

【0010】以上のように、この第1の実施形態では、次のような利点がある。

(i) n段の2分周回路2 0 - 1～2 0 - nにより、定常に存在する雑音を変換点のジッタとして増幅し、この増幅されたジッタにより、D - F F 3 0でOSC 1 0の出力信号S 1 0をサンプリングし、該D - F F 3 0のデータ出力端子Qから、“0”又は“1”的乱数化された乱数データを outputする構成になっている。そのため、電源投入後の一定時間後に、例えば、暗号化のためにCPU等で乱数データを読みむようにしても、この読み込みタイミングによる規則性が発生することなく、電源投入毎に新しい乱数データが得られる。従つて、装置の未使用時には電源を断にすることができるようになり、

装置の電池駆動時において電池寿命を長くすることができ、低消費電力化が可能となる。

(ii) 抵抗2 1及びコンデンサ2 2からなるC R 積分回路を用いて、ジッタを有する三角波状の積分信号S 2 2を生成し、これをD - F F 2 3で波形整形してクロック信号を生成しているので、ジッタを含んだクロック信号を簡単かつ的確に生成できる。

【0011】第2の実施形態

図6は、本発明の第2の実施形態を示す乱数発生回路の構成図であり、第1の実施形態を示す図1中の要素と共通の要素には共通の符号が付されている。この乱数発生回路では、図1の1つのOSC 1 0に代えて、非同期に動作する2つの第1の発振手段（例えば、OSC）1 0 - 1及び第2の発振手段（例えば、OSC）1 0 - 2を設け、この第1のOSC 1 0 - 1から出力される出力信号S 1 0 - 1をD - F F 3 0のデータ入力端子Dへ与え、第2のOSC 1 0 - 2の出力信号S 1 0 - 2を初段の2分周回路2 0 - 1内の抵抗2 1へ与え、出力データDAである乱数データを取出すD - F F 3 0の入力データと入力クロックとを非同期にする構成になっている。第2のOSC 1 0 - 2は、第1のOSC 1 0 - 1に対して非整数倍の周波数で発振し、また、この発振周波数の安定度が低く、ジッタも大きい低精度の回路構成にすることが望ましい。このようなOSC 1 0 - 2を用いる理由は、発振周波数の安定度が低いためにジッタが発生しやすく、この結果、D - F F 3 0で取出された乱数データの信頼度が向上するからである。

【0012】この第2の実施形態の乱数発生回路では、電源が投入されると、第1、第2のOSC 1 0 - 1、1 0 - 2が非同期で発振動作し、該第1のOSC 1 0 - 1の出力信号S 1 0 - 1が、D - F F 3 0のデータ入力端子Dへ送られ、さらに、該第2のOSC 1 0 - 2の出力信号S 1 0 - 2が、初段の2分周回路2 0 - 1へ送られる。初段の2分周回路2 0 - 1では、OSC 1 0 - 2自身のジッタを含んだ出力信号S 1 0 - 2を増幅する形で、クロック信号からなる出力信号S 2 3を後段の2分周回路2 0 - 2～2 0 - nへ順次送る。そのため、出力信号S 1 0 - 2に含まれたジッタが順次増大していき、出力信号S 1 0 - 1の半周期よりも大きなジッタ幅を有するクロック信号S 2 0が、最終段の2分周回路2 0 - nから出力され、D - F F 3 0のクロック入力端子Tへ送られる。D - F F 3 0では、クロック信号S 2 0に基づき、OSC 1 0 - 1の出力信号S 1 0 - 1を非同期でサンプリングし、出力データDAつまり乱数データを outputする。

【0013】この第2の実施形態では、第1の実施形態の利点を有する他に、さらに次のような利点も有する。

(iii) 第1の実施形態では、OSC 1 0という発振源が1つであるため、D - F F 3 0へのデータ入力とクロック入力が同期している。そのため、ジッタの分布によ

っては“0”や“1”的連続が発生し、得られた乱数データとしては信頼性が低くなる場合がある。そこで、この第2の実施形態では、発振源をOSC10-1と10-2の2つに分け、D-FF30へのデータ入力とクロック入力を非同期とし、クロック信号S20に含まれるジッタも、低精度のOSC10-2を用いることによって該ジッタを増大している。従って、第1の実施形態に比べ、乱数データがより確実に得られる。

【0014】第3の実施形態

図7は、本発明の第3の実施形態を示す乱数発生回路の構成図である。この乱数発生回路では、第1又は第2の実施形態に対してさらに乱数化を確実にするために、第1の実施形態又は第2の実施形態の乱数発生回路40の出力側に、さらにスクランブル回路50を接続している。このスクランブル回路50は、乱数発生回路40内のD-FF30から出力された出力データDAをさらにランダム化して乱数データDATを出力する機能を有し、例えば、生成多項式が $1 + X^{-6} + X^{-7}$ の回路で構成されている。

【0015】スクランブル回路50は、例えば、生成多項式が $1 + X^{-6} + X^{-7}$ の場合、2つの排他的論理和ゲート(以下、「Ex-OR」という)51、53、及び1つのシフトレジスタ52で構成されている。Ex-OR51の2つの入力端子のうち、一方の入力端子が、乱数発生回路40内のD-FF30のデータ出力端子Qに接続され、他方の入力端子が、他のEx-OR53の出力端子に接続されている。Ex-OR51の出力端子は、乱数データDATを出力する端子であり、シフトレジスタ52のデータ入力端子Dに接続されている。シフトレジスタ52のクロック入力端子Tには、乱数発生回路40から出力されたクロック信号S20が入力され、該シフトレジスタ52の2つのデータ出力端子Q6、Q7が、Ex-OR53の2つの入力端子に接続されている。この第3の実施形態の乱数発生回路では、電源投入によって乱数発生回路40から出力データDA及びクロック信号S20がが出力され、該出力データDAがスクランブル回路50へ送られる。スクランブル回路50内のEx-OR51は、2入力信号が不一致のときに出力信号が“1”、該2入力信号が一致するときには出力信号が“0”となり、これらの出力信号がシフトレジスタ52のデータ入力端子Dへ送られる。シフトレジスタ52では、クロック入力端子Tに入力されるクロック信号S20に応答して、Ex-OR51の出力信号を順次取込んでシフトしていく、2つのデータ出力端子Q6、Q7から出力する。この2つのデータ出力端子Q6、Q7の出力信号は、Ex-OR53に入力され、該Ex-OR53の出力信号がEx-OR51の入力端子にフィードバックされる。これにより、Ex-OR51の出力端子から、生成多項式 $1 + X^{-6} + X^{-7}$ で表わされるスクランブル回路50によりランダム化された乱数データDAT

が出力される。

【0016】この第3の実施形態では、第1及び第2の実施形態の利点を有する他に、さらに次のような利点も有する。

(iv) 第2の実施形態のように、2つのOSC10-1、10-2を設けたとしても、これらの発振周波数の変動によって該OSC10-1と10-2が互いに整数倍の周波数比になってしまふ場合があり得る。このような場合でも、“0”又は“1”的連続発生を、付加したスクランブル回路50によってランダム化しているので、乱数データDATを第2の実施形態よりもより確実に得られる。なお、本発明は上記実施形態に限定されず、種々の変形が可能である。この変形例としては、例えば次のようなものがある。

【0017】(a) 図1及び図6の各2分周回路20-1～20-nは、抵抗21及びコンデンサ22からなるCR積分回路と、D-FF23からなる2分周カウンタとで構成しているが、このCR積分回路を他の回路で構成したり、あるいは2分周回路を他のフリップフロップ回路等で構成してもよい。さらに、n段の2分周回路20-1～20-nで構成されるクロック生成手段は、ジッタを含んだクロック信号を生成し、このジッタを増幅する回路であるから、このような機能を実行できる他の回路構成に変更してもよい。また、D-FF30は、他のフリップフロップ回路等のサンプリング手段で構成してもよい。

(b) 図7のスクランブル回路50は、生成多項式が $1 + X^{-6} + X^{-7}$ の回路で構成したが、これらの段数を増やすことによって他の生成多項式の回路構成にすることにより、スクランブルの精度をより向上できる。また、これらのスクランブル回路50は、図示以外の回路で構成してもよい。

(c) 上記実施形態では、伝送データの暗号化のための乱数発生回路について説明したが、これらの乱数発生回路は暗号化以外の他の種々の用途に用いることができる。

【0018】

【発明の効果】以上詳細に説明したように、第1、第4及び第5の発明によれば、クロック生成手段によって定常に存在する雑音をジッタとして増幅し、この増幅されたジッタを有するクロック信号をサンプリング手段に与え、該サンプリング手段によって発振手段の出力信号をサンプリングし、乱数データを取出すようにしているので、例えば、電源投入後の一定時間後に該乱数データを暗号化等のために読み込むようにしても、この読み込みタイミングによる規則性が発生することなく、電源投入毎に新しい乱数データが得られる。従って、装置の未使用時には電源を断つことができるようになり、例えば、装置の電池駆動時において電池寿命を長くすることができ、低消費電力化が可能となる。第2、第4及び第

5の発明によれば、精度の異なる2つの第1及び第2の発振手段を設け、サンプリング手段へのデータ入力とクロック入力を非同期の構成にしたので、第1の発明に比べて乱数データをより確実に得られる。第3の発明によれば、第1又は第2の発明の乱数発生回路の出力側にスクランブル回路を設けたので、第1又は第2の発明で得られた乱数データをさらにランダム化することにより、第2の発明に比べて乱数データをより確実に得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示す乱数発生回路の構成図である。

【図2】従来の乱数発生回路の構成図である。

【図3】図2の暗号化処理を示す図である。

【図4】図1の動作波形図である。

【図5】図1の動作波形図である。

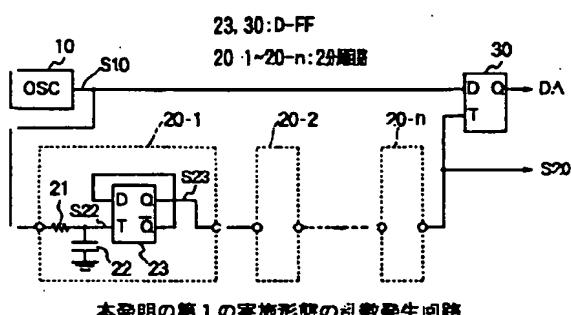
【図6】本発明の第2の実施形態を示す乱数発生回路の構成図である。

【図7】本発明の第3の実施形態を示す乱数発生回路である。

【符号の説明】

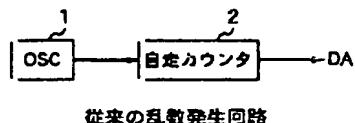
10, 10-1, 10-2	OSC (発振回路)
20-1~20-n	2分周回路
21	抵抗
22	コンデンサ
23, 30	D-FF
40	乱数発生回路
50	スクランブル回路

【図1】



本発明の第1の実施形態の乱数発生回路

【図2】



従来の乱数発生回路

【図3】

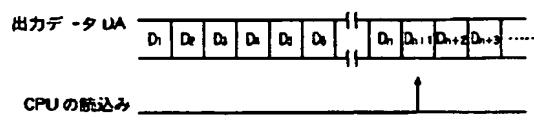


図2の暗号化処理

【図4】

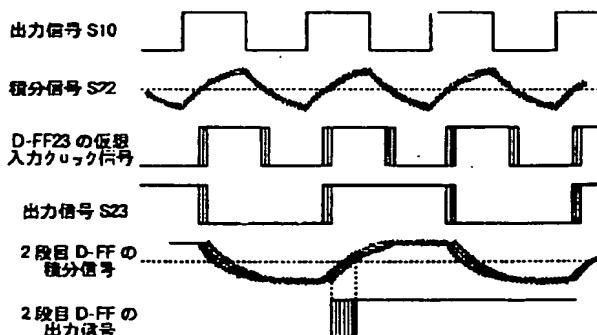


図1の動作波形

【図5】

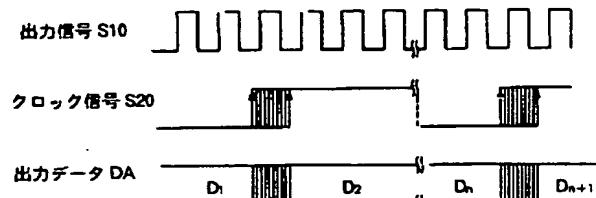
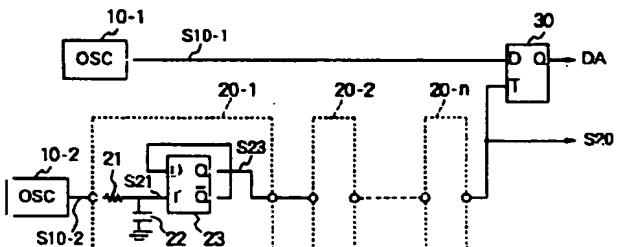


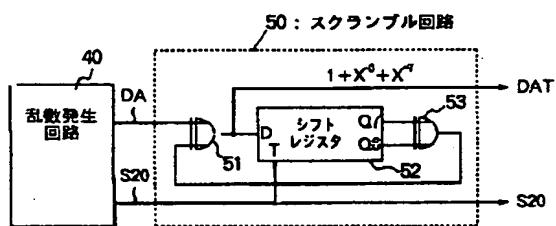
図1の動作波形

【図6】



本発明の第2の実施形態の乱数発生回路

【図7】



本発明の第3の実施形態の乱数発生回路